



**【特許請求の範囲】****【請求項 1】**

ユーザを直接的に特定可能な第 1 ユーザ情報を利用して、グリッド環境の利用を許可すべきユーザであるか否かを判断する認証部と、

前記ユーザの認証に成功した場合、前記第 1 ユーザ情報とは無関係に予め用意された第 2 ユーザ情報に基づいて、前記グリッド環境において利用されるプロキシ証明書を作成する生成部と、

前記プロキシ証明書を利用して、前記グリッド環境における所定の処理を行う計算機に利用許可を要求する要求部と、

を備えることを特徴とする管理装置。

10

**【請求項 2】**

複数のそれぞれ異なる前記第 2 ユーザ情報を保持する匿名ユーザ情報格納部を更に備え、前記生成部は前記匿名ユーザ情報格納部に保持されている第 2 ユーザ情報のいずれかひとつを利用して前記プロキシ証明書を作成することを特徴とする請求項 1 に記載の管理装置。

**【請求項 3】**

前記認証部において認証に成功した第 1 ユーザ情報と、プロキシ証明書の生成に利用した第 2 ユーザ情報とを対応付けるマッピング処理部と、

マッピングした第 1 ユーザ情報と第 2 ユーザ情報とを対応付けて保持するマッピングテーブルと、

所定の第 2 ユーザ情報に対応付けられて前記計算機から提供された前記所定の処理の実行結果を受け付ける処理結果受付部と、

前記マッピングテーブルを参照して、前記実行結果に対応付けられた前記所定の第 2 ユーザ情報に対応する第 1 ユーザ情報を特定し、その第 1 ユーザ情報で特定されるユーザに前記実行結果を提供するジョブ管理部と、

を更に備えることを特徴とする請求項 1 または 2 に記載の管理装置。

20

**【請求項 4】**

第 2 ユーザ情報に対応付けられた第 1 ユーザ情報で特定される所定のユーザに関する情報の提供要求を前記計算機から受け付け、その提供要求に応じて、前記所定のユーザに関する属性情報を前記計算機に送信する応答部を更に備えることを特徴とする請求項 1 から 3 のいずれかに記載の管理装置。

30

**【請求項 5】**

前記計算機に提供可能な前記属性情報のリストを保持する属性リスト格納部を更に備え、

前記応答部は、前記計算機に要求された場合に、前記リストの情報を送信することを特徴とする請求項 4 に記載の管理装置。

**【請求項 6】**

前記応答部は、前記所定のユーザに関する詳細なユーザ情報を一般化して生成された前記属性情報を前記計算機に送信することを特徴とする請求項 4 または 5 に記載の管理装置。

40

**【請求項 7】**

前記実行結果を所定の第 2 ユーザ情報に対応付けて格納する結果格納部と、

前記計算機から所定の第 2 ユーザ情報に対応付けられた実行結果を要求された場合、前記結果格納部に保持されている前記所定の第 2 ユーザ情報に対応付けられた前記実行結果をその計算機に提供するファイル管理部と、

を更に備えることを特徴とする請求項 3 から 6 のいずれかに記載の管理装置。

**【発明の詳細な説明】****【技術分野】****【0001】**

この発明はグリッドコンピューティング技術に関し、とくにグリッド環境において認証

50

を行う装置およびシステムに関する。

【背景技術】

【0002】

ネットワーク技術が発達することにより、例えば電子メールが日常的に利用され、また様々なウェブサイトが多種多様なサービスを提供し、利用されている。このようなネットワークの利用は、今や当然の情報取得手段として我々の日々の生活に浸透しつつある。ネットワーク技術の発達にともない、様々な機器がネットワークに接続されるようになった。こうした中、グリッドコンピューティングと呼ばれる計算機の利用形態が生まれた。グリッドコンピューティングは、ネットワークを介して複数のコンピュータ資源を接続することにより、高性能なコンピュータを仮想的に形成し、ユーザが必要とする処理能力を提供することができる。グリッドコンピューティングを実現するシステムを、以下、「グリッドシステム」という。また、グリッドシステムが提供し、ユーザが享受するサービス環境を「グリッド環境」という。

10

【0003】

図1(a)は、従来のグリッドシステム10の構成図である。第1計算機20a、第2計算機20b、および第3計算機20c(以下、単に「計算機20」という)は、例えば所定の企業や研究所のコンピュータであり、グリッドシステム10におけるコンピュータ資源として利用される。一般にそれぞれの計算機20は、独立して機能し、独自のユーザ認証システムを有する。このため、ユーザは、利用する計算機20毎に認証作業を行う必要がある。この認証処理は、PKI(Public Key Infrastructure)に基づいており、認証局14が発行したユーザ証明書を利用して行われる。この認証処理の過程で、グリッドシステム10はユーザにパスフレーズの入力を要求する。パスフレーズは、暗号化されたユーザの秘密鍵を復号するために利用され、その役割の重要さからビット数が長くなっている。そもそも、グリッドシステムは、複数の計算機20を同時に利用して、一台の計算機20では得られない高速な処理を実現することをひとつの目的としており、ひとつのジョブを実行するために複数の計算機20を利用することが多い。このため、ユーザは、利用する計算機20毎に、認証処理のためにパスフレーズを入力する必要があるが生じてしまう。この認証処理は、ユーザに対してかなりの負担になる。そこで、グリッドシステムでは証明書の連鎖を用いている。すなわち、ユーザによって発行された証明書を持っているものはそのユーザの権限を持っており、自分自身の証明書を発行することができる。これをプロキシ証明書と呼び、ユーザ証明書の代わりとする。プロキシ証明書の有効期限を短くする代わりに、それを暗号化せずにファイルに保存するようにしているため、パスフレーズの再入力なしに計算機間でユーザの認証が可能である。

20

30

【0004】

一方、ユーザにとって、グリッドシステムの利用には、グリッドシステムについての知識を必要とする。そこで、グリッドシステムについての十分な知識がなくてもグリッドシステムを容易に利用可能とする目的で管理装置30が設けられている場合が多い。管理装置30は、グリッドシステムにおける各計算機20のポータルサイトとして機能するグリッドポータルであり、クライアント装置40が生成したプロキシ証明書44を利用して代理的にそれぞれの計算機20に対して認証処理を行う。これにより、ユーザは利用する計算機20毎に、自ら認証処理を行わなくて済む。また、管理装置30は、ユーザからクライアント装置40を介して指定された処理内容に応じて、処理に利用する計算機20を選択し、選択した計算機20に対して認証処理を行う。

40

【0005】

クライアント装置40は、ユーザが操作する端末装置であり、プロキシ証明書44を発行し管理装置30に提供するとともに、計算機20に対する処理内容を管理装置30に指示する。プロキシ証明書44を発行し管理装置30に提供する機能と、計算機20に対する処理内容を管理装置30に指示する機能とはそれぞれ異なる装置で提供されてもよいし、同一の装置で提供されてもよい。クライアント装置40は、プロキシ証明書44を生成するためのプロキシ証明書生成部42を有する。グリッドシステム10の利用にあたり、

50

最初に、ユーザは、プロキシ証明書生成部 4 2 を利用して、プロキシ証明書 4 4 を生成する。そして、クライアント装置 4 0 と管理装置 3 0 との間で委譲 (delegation) が行われることにより、管理装置 3 0 上にユーザのプロキシ証明書が生成される。その後、クライアント装置 4 0 は、ウェブブラウザを利用して管理装置 3 0 にアクセスし、サービス画面を表示する。管理装置 3 0 は、クライアント装置 4 0 からのプロキシ証明書 4 4 を保持し、必要に応じて認証処理に利用することができる。

#### 【0006】

具体的には、プロキシ証明書生成部 4 2 は、Globus toolkit により実現され、管理装置 3 0 は、Myproxy server により実現される。クライアント装置 4 0 において、コマンド「grid-proxy-init」が実行されると Globus toolkit はプロキシ証明書 4 4 を生成する。そして、コマンド「myproxy-init」が実行されると、管理装置 3 0 は新しい公開鍵と秘密鍵のペアを作成し、その公開鍵をもとに CSR (Certificate Signing Request) を作成してクライアント装置 4 0 に送信する。クライアント装置 4 0 では予め生成しておいた一時秘密鍵 (クライアント側で予め生成されているプロキシ証明書に格納されている公開鍵に対応する秘密鍵) で CSR に署名をしたものと、予め作成しておいたプロキシ証明書のベースになるファイル 7 0 を管理装置 3 0 に送信する。管理装置 3 0 はクライアントから送られてきたファイル 7 0 に一時秘密鍵を添付することにより、管理装置 3 0 にプロキシ証明書が作成される。そして、管理装置 3 0 の Myproxy server にプロキシ証明書 4 4 が格納される。Myproxy server はグリッドポータルである管理装置 3 0 上で動作してもよいし、管理装置 3 0 とは異なる装置上で動作してもよい。いずれの形態でも、Myproxy server が動作する装置と管理装置 3 0 との間で委譲が行われることにより、管理装置 3 0 上にユーザのプロキシ証明書 4 4 が生成される。

#### 【0007】

図 1 (b) は、プロキシ証明書ファイル 7 0 のデータ構造と生成処理を説明するための図である。図 1 (a) のプロキシ証明書生成部 4 2 は、図 1 (a) の認証局 1 4 が発行したユーザ証明書 5 0 と、秘密鍵 5 2 とに基づいて、プロキシ証明書ファイル 7 0 を発行する。プロキシ証明書生成部 4 2 は、一時的に利用する一時秘密鍵 7 4 と一時公開鍵 7 6 とを生成する。そして、プロキシ証明書生成部 4 2 は、一時公開鍵 7 6 をユーザ秘密鍵 5 2 で署名、つまり暗号化する。このとき、暗号化されたユーザ秘密鍵 5 2 を復号する必要があるため、ユーザは一度だけパスフレーズ 5 4 を入力する。

#### 【0008】

プロキシ証明書 4 4 は、一時公開鍵 7 6 をユーザ秘密鍵 5 2 で署名したものであり、プロキシ証明書 4 4 にユーザ証明書 5 0 を添付することで、プロキシ証明書 4 4 の正当性が保証され、かつユーザ証明書 5 0 の正当性は図 1 (a) の認証局 1 4 により保証される。そして、このように保証された一時公開鍵 7 6 に対応する一時秘密鍵 7 4 も正当性が保証される。

#### 【0009】

ここで、一時秘密鍵 7 4 は、ユーザ秘密鍵 5 2 のようにパスフレーズ 5 4 で暗号化されていない。これにより、管理装置 3 0 は、ユーザからパスフレーズ 5 4 を受け付けることなく、計算機 2 0 に対する認証処理が可能になる。プロキシ証明書ファイル 7 0 は、プロキシ証明書 4 4、一時秘密鍵 7 4、およびユーザ証明書 5 0 を含む。図 1 (a) のクライアント装置 4 0 と管理装置 3 0 との間では委譲を行うことにより、管理装置 3 0 上にユーザのプロキシ証明書が生成される (非特許文献 1)。

【非特許文献 1】「ハイパフォーマンスコМПユーティングシステム」、情報処理学会論文誌 Vol. 43、No. SIG6 (HPS5)、p172 - p183、2002 年

#### 【発明の開示】

#### 【発明が解決しようとする課題】

#### 【0010】

図 1 (a) のプロキシ証明書生成部 4 2 は、所定のプログラムを実行することによりクライアント装置 4 0 に形成される。そのため、ユーザはそのプログラムをクライアント装

10

20

30

40

50

置 40 に予めインストールする必要がある。また、グリッドシステム 10 を利用する前に、プロキシ証明書ファイル 70 を生成するためのコマンドを実行し、その後、プロキシ証明書ファイル 70 を管理装置 30 に送信するためのコマンドを実行する必要がある。これらの作業は、コマンドプロンプトを利用して行われる。

【0011】

グリッドコンピューティングは、UNIX（登録商標）や LINUX などの OS を利用して、各種の研究や開発を行う研究者や技術者により利用されてきた。このため、グリッド環境は、例えばコマンドプロンプトを利用してコマンドを実行するという作業に慣れたユーザに多く利用されており、一般ユーザの利用という観点からの考察が十分に行われていなかった。

10

【0012】

本発明者は、例えば電子メールが日常的に利用されている様に、今後グリッド環境が日常的に利用されることを考えた場合、コマンドプロンプトを利用する形態では一般ユーザに負担をかけるとともに、一般ユーザへの普及も望めないと考えた。更に、本発明者は、グリッドコンピューティングが普及し、例えば企業などが新しい商品の研究や、コンピュータグラフィックなど、非常に重要で極秘に取り扱われるべき情報を扱うことを考慮し、セキュアなグリッド環境を提供する必要があると考え、本発明に想到した。

本発明は上記課題に鑑みてなされたものであり、その目的は、グリッド環境における認証処理を容易にする技術、セキュアなグリッド環境を実現する技術を提供することにある。

20

【課題を解決するための手段】

【0013】

本発明のある態様は、グリッド・コンピューティングシステムにおけるポータルサイトとして機能する管理装置に関する。この装置は、ユーザを直接的に特定可能な第 1 ユーザ情報を利用して、グリッド環境の利用を許可すべきユーザであるか否かを判断する認証部と、ユーザの認証に成功した場合、第 1 ユーザ情報とは無関係に予め用意された第 2 ユーザ情報に基づいて、グリッド環境において利用されるプロキシ証明書を生成する生成部と、プロキシ証明書を利用して、グリッド環境における所定の処理を行う計算機に利用許可を要求する要求部とを備える。計算機は、第 1 ユーザ情報とは無関係の第 2 ユーザ情報に基づいて生成されたプロキシ証明書に基づいて認証を行うので、ユーザの個人情報に計算機に伝達されることを防止でき、計算機に対して匿名性を確保できる。

30

【0014】

この装置は、複数のそれぞれ異なる第 2 ユーザ情報を保持する匿名ユーザ情報格納部を更に備え、生成部は匿名ユーザ情報格納部に保持されている第 2 ユーザ情報のいずれかひとつを利用してプロキシ証明書を生成してもよい。これにより、それぞれ異なる匿名ユーザに署名されたプロキシ証明書をユーザ毎に生成することができる。

【0015】

この装置は、認証部において認証に成功した第 1 ユーザ情報と、そのユーザのプロキシ証明書の生成に利用した第 2 ユーザ情報とを対応付けるマッピング処理部と、マッピングした第 1 ユーザ情報と第 2 ユーザ情報とを対応付けて保持するマッピングテーブルと、所定の第 2 ユーザ情報に対応付けられて計算機から提供された所定の処理の実行結果を受け付ける処理結果受付部と、マッピングテーブルを参照して、実行結果に対応付けられた所定の第 2 ユーザ情報に対応する第 1 ユーザ情報を特定し、その第 1 ユーザ情報で特定されるユーザに実行結果を提供するジョブ管理部とを更に備えてもよい。これにより、第 2 ユーザ情報に対応付けられた実行結果を、本来の依頼元であるユーザに提供することができる。

40

【0016】

この装置は、第 2 ユーザ情報に対応付けられた第 1 ユーザ情報で特定される所定のユーザに関係する情報の提供要求を計算機から受け付け、その提供要求に応じて、所定のユーザに関係する属性情報を計算機に送信する応答部を更に備えてもよい。これにより、匿名

50

性を確保するとともに、ユーザの属性に応じたサービスを提供可能になる。

【0017】

この装置は、計算機に提供可能な属性情報のリストを保持する属性リスト格納部を更に備えてよく、応答部は、計算機に要求された場合に、そのリストの項目を送信してもよい。これにより、提供可能な属性情報を計算機に予め通知できる。

【0018】

応答部は、所定のユーザに関係する詳細なユーザ情報を一般化して生成された属性情報を計算機に送信してもよい。一般化することにより、属性情報に基づいて、ユーザを類推することを困難にできる。

【0019】

この装置は、実行結果を所定の第2ユーザ情報に対応付けて格納する結果格納部と、計算機から所定の第2ユーザ情報に対応付けられた実行結果を要求された場合、結果格納部に保持されている所定の第2ユーザ情報に対応付けられた実行結果をその計算機に提供するファイル管理部とを更に備えてもよい。これにより、グリッド環境における複数の計算機を利用してジョブを処理する場合に、匿名性を確保したまま所定の計算機による計算結果を他の計算機が再利用することができる。

【0020】

なお、以上の構成要素の任意の組合せ、本発明の表現を方法、装置、システム、記録媒体、コンピュータプログラムなどの間で変換したものもまた、本発明の態様として有効である。

【発明の効果】

【0021】

本発明によれば、グリッド環境における認証処理を容易にすることができ、利便的でセキュアな認証処理を実現する装置およびシステムを提供できる。

【発明を実施するための最良の形態】

【0022】

＜第1の実施の形態＞

図2は、第1の実施の形態に係るグリッドシステム600の構成図である。各構成要素は、ハードウェアコンポーネントで言えば、任意のコンピュータのCPU、メモリ、メモリにロードされた本図の構成要素を実現するプログラム、そのプログラムを格納するハードディスクなどの記憶ユニット、ネットワーク接続用インターフェース等を中心に実現されるが、その実現方法、装置にはいろいろな変形例があることは、当業者には理解されるところである。これから説明する各図は、ハードウェア単位の構成ではなく、機能単位のブロックを示している。

【0023】

クライアント装置200は、ユーザが操作する端末装置であり、ネットワークを介して管理装置610に接続している。管理装置610は、クライアント装置200を操作するユーザを認証する。そして、認証に成功した場合、そのユーザに依頼された処理を計算機400に実行させる。計算機400は、ネットワークを介して管理装置610と接続しており、管理装置610を認証する。そして、認証に成功した場合、計算機400は、管理装置610から指示された処理を実行する。

【0024】

管理装置610は、認証部612、ユーザ情報格納部614、プロキシ証明書生成部616、および匿名情報格納部618を有する。ユーザ情報格納部614は、例えば、ユーザを識別する情報（以下、単に「実ユーザID」という）およびパスワードの組合せなど、グリッドシステム600の利用を許可すべきユーザを認証するための、ユーザに直接関係する情報（以下、単に「実認証情報」という）を保持する。認証部612は、ユーザ情報格納部614に保持されている実認証情報に基づいて、クライアント装置200を操作するユーザの認証を行う。認証部612は、例えばSSL（Secure Socket Layer）でクライアント装置200と接続し、ユーザから実ユーザIDとパスワードを受け付けて認証

10

20

30

40

50

を行ってもよいし、ユーザから所定の認証局が発行したユーザ証明書を受け付けて、そのユーザ証明書に基づいて認証を行ってもよい。つまり認証部 6 1 2 は、クライアント装置 2 0 0 を操作するユーザを直接的に特定可能な情報を用いて認証を行う。そして、認証に成功した場合、認証部 6 1 2 はプロキシ証明書の発行をプロキシ証明書生成部 6 1 6 に指示する。

#### 【0025】

匿名情報格納部 6 1 8 は、管理装置 6 1 0 が管理する計算機 4 0 0 を利用するための識別情報を保持する。この識別情報は、クライアント装置 2 0 0 のユーザとは無関係に、計算機 4 0 0 に予め登録された情報である。つまり、この識別情報は、管理装置 6 1 0 の管理者と計算機 4 0 0 の管理者との間で結ばれた契約に基づいて登録されたものであり、実際のユーザ情報の代わりに利用する実際のユーザとは無関係の情報（以下、単に「匿名情報」という）である。匿名情報は、匿名ユーザ名、公開鍵、秘密鍵、認証局による証明書（以下、単に「匿名証明書」という）などを含む。また、匿名情報格納部 6 1 8 は、単一の匿名情報だけを保持してもよいし、複数の異なる匿名情報を保持してもよい。

10

#### 【0026】

プロキシ証明書の発行を指示された場合、プロキシ証明書生成部 6 1 6 は、匿名情報格納部 6 1 8 に保持されている匿名情報を利用して、匿名プロキシ証明書 6 2 0 を生成する。この匿名プロキシ証明書 6 2 0 は、図 1 (b) を用いて説明したプロキシ証明書と同一のデータ構造をしており、匿名情報格納部 6 1 8 に保持されている匿名情報で署名されている。管理装置 6 1 0 は、この匿名プロキシ証明書 6 2 0 を用いて、計算機 4 0 0 に対する認証処理を行い、計算機 4 0 0 に所定の処理を実行させる。

20

#### 【0027】

このように、管理装置 6 1 0 がユーザに対しては実認証情報に基づいて認証を行い、計算機 4 0 0 に対する指示は匿名情報を利用して行うことで、管理装置 6 1 0 はユーザに依頼された処理を計算機 4 0 0 に匿名で実行させることができる。これにより、処理内容の依頼者つまりユーザの秘匿性を保つことができ、ユーザの個人情報がネットワークに流れることを最小限に抑えることができる。また、認証部 6 1 2 が、ユーザ ID とパスワードによるベーシック認証を行うことにより、ユーザはクライアント装置 2 0 0 にプロキシ証明書を生成するための専用プログラムを予めインストールし、毎回その専用プログラムを実行するといった作業が不要になる。これにより、グリッドシステム 6 0 0 を利用するための認証処理を簡便にすることができる。

30

#### 【0028】

グリッド環境における処理の匿名性は、匿名情報格納部 6 1 8 がひとつの匿名情報を保持することで実現することができる。しかしながら、ユーザ毎に異なるサービスを提供したり、ユーザ毎に使用料金を設定したりすることは、ひとつの匿名情報だけでは困難である。そこで、以下に複数の匿名情報を利用することにより、匿名性を確保しつつ、ユーザ毎にサービスを提供可能にする形態を説明する。

#### 【0029】

< 第 2 の実施の形態 >

第 2 の実施の形態の要素技術は主に 3 つある。第 1 の技術は「複数の匿名情報を利用して、ユーザ毎に匿名プロキシ証明書を発行する技術」である。第 2 の技術は「ユーザ毎にサービス内容を変えてきめ細かなサービスを提供するために、匿名性を保ちながらユーザの属性を提供する技術」である。第 3 の技術は「匿名性を保ちながら過去の計算結果を使用する、もしくは他のユーザに公開するといったデータの再利用を可能にする技術」である。まず、これらの要素技術について説明する。

40

#### 【0030】

図 3 は、第 1 の要素技術である「複数の匿名情報を利用して、ユーザ毎に図 2 の匿名プロキシ証明書 6 2 0 を生成する技術」を説明するための図である。グリッドポータルサイトとして機能する管理装置 1 0 0 は、匿名情報を複数保持し、それぞれのユーザ 6 3 0 に対応して、匿名プロキシ証明書 6 2 0 を生成する。その匿名プロキシ証明書 6 2 0 は、匿

50

名情報に含まれる匿名ユーザにより署名されている。そして、管理装置 100 は各ユーザ 630 からの処理内容に基づいて、その処理に適した適当なサーバ 632 をグリッド環境の中から選択し、処理を指示する。サーバ 632 は、匿名プロキシ証明書 620 の発行者である匿名ユーザの匿名ユーザ証明書に基づいて、認証を行う。そして、認証に成功した場合、サーバ 632 はリソースを割り当て、プロセスを実行する。これにより、ユーザ 630 毎に匿名プロキシ証明書 620 を生成できるので、各ユーザ 630 と匿名ユーザとを一対一に対応付けて、グリッド環境における処理を管理することができる。

#### 【0031】

図 4 は、第 2 の要素技術である「匿名性を保ちながらユーザの属性を提供する技術」を説明するための図である。管理装置 100 は、ユーザ 630 のユーザ属性証明書 634 を生成する。そして、管理装置 100 は、そのユーザ属性証明書 634 をユーザ 630 に対応付けられた匿名ユーザの属性として匿名属性証明書 636 に変換する。この匿名属性証明書 636 は、例えば年齢、性別、会員情報の有無、職種、居住地などのユーザ属性証明書 634 に含まれる個人情報をも一般化したデータを含み、グリッド環境におけるサービス内容に応じて任意に定義される。管理装置 100 は、プロセスの実行要求に先立ち、サーバ 632 に実行条件を打診する (S100)。サーバ 632 は、実行条件に基づいて、ユーザの属性を問い合わせる (S102)。そして、管理装置 100 は、その問い合わせに応じたユーザの属性をサーバ 632 に回答する (S104)。これにより、管理装置 100 は匿名性を保ちながら、ユーザの属性を提供することができる。この技術により、例えばサービス提供側すなわちサーバ 632 側がユーザの会員権や所属などの各種のユーザ属性に応じて、使用料金の割引や優先的に処理を行うことなど種々の特典を設定することができる。こうした特典により、サービス提供側は他との差別化を図ることができ、グリッド環境におけるビジネスに競争の原理を持ち込み、サービス提供者間の競争を激化し、グリッド環境そのものを活性化できる。

#### 【0032】

図 5 は、第 3 の要素技術である「匿名性を保ちながら過去の計算結果を使用する、もしくは他のユーザに公開するといったデータの再利用を可能にする技術」を説明するための図である。管理装置 100 は、ユーザ 630 に対する処理を実名に基づいて処理する実名処理部 102 と、匿名で処理する匿名処理部 104 とを備える。実名処理部 102 は、実認証情報に基づいて、ユーザ 630 の認証を行い、認証に成功した場合、実ユーザと匿名ユーザとを対応付けてマッピングする。匿名処理部 104 は、実ユーザにマッピングされた匿名ユーザの情報を利用して、匿名ユーザとしてサーバ 632 に所定の処理を依頼する。

#### 【0033】

サーバ 632 は、前述した匿名プロキシ証明書 620 に基づいて、匿名ユーザの認証を行う。そして、認証に成功した場合、サーバ 632 は、所定の処理を実行し、計算の途中で生成されたテンポラリ・ファイルなどを一時的なデータとして格納し、計算結果を管理装置 100 に提供する。そして、サーバ 632 は、例えば計算結果を管理装置 100 に提供したことを契機に、計算結果やテンポラリ・ファイルを消去する。これにより、サーバ 632 からの計算結果等の漏洩を防止もしくは抑制できる。管理装置 100 は、サーバ 632 から提供された計算結果を、匿名ユーザ名に基づいて短期間アクセス可能な短期保存データ 96 と、実ユーザ名に基づいて長期間アクセス可能な長期保存データ 94 とに分けて格納する。このように、管理装置 100 が実ユーザ名と匿名ユーザ名とのマッピングを解決し、計算結果などのデータへのアクセス制御を行う。これにより、匿名性を保ちつつ、データの再利用を可能にできる。

#### 【0034】

これら 3 つの要素技術を、グリッド環境において提供するサービス内容に応じて、適切に組合せることにより、グリッド環境におけるシングル・サインオンを実現し、セキュアで利便性の高い利用環境をユーザに提供するポータルサイト、つまり管理装置 100 を実現することができる。要素技術の組合せは任意であり、管理装置 100 に全ての要素技術



が組み込まれてもよいし、一部の要素技術が組み込まれてもよい。

#### 【0035】

図6は、第2の実施の形態に係るグリッドシステム500の構成図である。クライアント装置200は、ユーザが操作する端末装置であり、ネットワークを介して管理装置100に接続している。処理要求部202は、管理装置100に対してグリッド環境を利用した処理を要求する。こうした処理を以下、単に「ジョブ」という。データ格納部204は、ジョブの実行に必要な、例えば変数、物質、関数、汎用データベースの名称などを保持する。データ格納部204に保持されるデータは、グリッド環境において実行する処理の内容により異なる。処理要求部202は、データ格納部204に保持されているデータとともに、ジョブの実行を管理装置100に要求する。他の例では、処理要求部202は、直接ユーザからジョブの実行に必要なデータの入力を受け付けてもよい。また、処理要求部202は、ジョブの要求に先立ち、グリッド環境の利用の可否を実認証情報に基づいて行う。処理要求部202は、実際のユーザ情報を利用して管理装置100に対する種々の指示を行う。

10

#### 【0036】

一方、結果受付部206は、管理装置100からジョブを実行して得られた計算結果を受け付け、結果格納部208に格納する。表示処理部210は、結果格納部208に格納されている計算結果に基づいて、表示処理を行う。こうした、クライアント装置200における一連の処理は、例えば専用のネットワーククライアントで実現されてもよいし、ウェブブラウザなどの汎用的なネットワーククライアントで実現されてもよい。好ましくは、ウェブブラウザで実現される形態である。

20

#### 【0037】

管理装置100は、クライアント装置200を操作するユーザを、実認証情報に基づいて認証し、匿名ユーザからの依頼としてアプリケーション提供装置300にジョブを依頼する。管理装置100は、主にユーザの実名に基づいて、認証処理や属性情報に関する処理を行う実名処理部102、ユーザの情報を匿名に変えて、匿名にてアプリケーション提供装置300に対して認証処理を行う匿名処理部104、および匿名でジョブの実行を指示し、その計算結果を管理するジョブ管理部110を有する。匿名情報生成部106は、図3を用いて説明した第1の要素技術を実現するブロックであり、アプリケーション提供装置300および計算機400に対して処理を指示するための匿名情報すなわち匿名プロキシ証明書を生成する。

30

#### 【0038】

属性情報管理部108は、図4を用いて説明した第2の要素技術を実現するブロックであり、匿名の属性情報を管理する。属性情報管理部108は、アプリケーション提供装置300との間で、ユーザの所属や権利などに応じた使用料金などの、アプリケーション提供装置300および計算機400の利用に関わる条件交渉を、匿名属性情報を用いて行う。これにより、属性情報管理部108は匿名にて、ユーザの属性に応じた条件交渉を行うことができる。

#### 【0039】

ジョブ管理部110はアプリケーション提供装置300から計算結果を受け付け、それを管理装置100の一時格納部112に格納するとともに、クライアント装置200と接続して計算結果を提供する。管理装置100の削除部114は、計算結果をクライアント装置200に提供したことを検出すると、一時格納部112に保持されている計算結果を削除する。他の例で、削除部114は、計算結果の提供前であっても、所定の時間が経過した場合、一時格納部112から計算結果を削除してもよい。このように、管理装置100は、クライアント装置200とは、ユーザの実名に基づいて通信を行い、アプリケーション提供装置300とは匿名すなわち間接的なユーザの情報に基づいて通信を行う。これにより、アプリケーション提供装置300に対しては、ユーザの個人情報を隠蔽することができる。

40

#### 【0040】

50

アプリケーション提供装置 300 は、複数の計算機 400 を配下に有し、例えばジョブの内容や各計算機 400 におけるジョブの実行状態すなわち計算機 400 の稼働状態に応じて、ジョブを振り分ける。そして、アプリケーション提供装置 300 は、計算結果を計算機 400 から受け付け、管理装置 100 に中継する。

#### 【0041】

匿名認証部 302 は、管理装置 100 がユーザの実名の代わりに利用する匿名ユーザの認証を行う。指示部 304 は、ジョブの内容を受け付け、そのジョブを実行するためのプログラムをアプリケーション格納部 306 から読み込む。そして、指示部 304 は、そのプログラムとともに、ジョブの実行を計算機 400 に指示する。アプリケーション提供装置 300 が計算機 400 にジョブの実行を指示する前段に、匿名プロキシ証明書を利用して委譲による認証が行われる。匿名プロキシ証明書には、ユーザに関する情報が含まれていないため、委譲された全ての計算機にユーザの個人情報が渡されることはない。

10

#### 【0042】

中継部 308 は、計算結果を計算機 400 から受け付け、アプリケーション提供装置 300 の一時格納部 312 に格納する。そして、中継部 308 は、計算結果を管理装置 100 に提供する。つまり、中継部 308 は、計算機 400 がジョブを実行することにより算出した計算結果を管理装置 100 に中継する。削除部 310 は、計算結果の提供が完了したことを契機として、一時格納部 312 に一時的に格納されている計算結果を削除する。このように、計算結果を積極的に削除することにより、アプリケーション提供装置 300 を介して計算結果が漏洩することを防止できる。

20

#### 【0043】

計算機 400 は、ジョブを実際に処理し、計算結果をアプリケーション提供装置 300 に提供する。また、計算機 400 は、必要に応じて汎用データ提供装置 250 に保持されている汎用データを利用して、ジョブを処理する。汎用データ提供装置 250 は、汎用データを汎用データ格納部 252 に保持しており、例えば遺伝子情報、物性情報、気象情報など各種のデータを保持するデータベースであってよい。

#### 【0044】

処理要求受付部 402 は、アプリケーション提供装置 300 から匿名にてジョブを受け付け、ジョブを実行するためのプログラムを実行部 404 に供給する。この処理の前段として、アプリケーション提供装置 300 から委譲された匿名プロキシ証明書を受け付け、委譲による認証処理が行われる。取得部 406 は、そのプログラムが必要とする汎用データを汎用データ提供装置 250 から取得し、実行部 404 に供給する。実行部 404 は、プログラムを実行し、実行結果を計算結果として提供部 408 に出力する。提供部 408 は、計算結果を一時格納部 410 に格納するとともに、アプリケーション提供装置 300 に提供する。計算機 400 の削除部 412 は、計算結果の提供が完了したことを契機として、一時格納部 410 に一時的に格納されている計算結果を削除する。このように、計算結果を積極的に削除することにより、計算機 400 を介して計算結果が漏洩することを防止できる。

30

#### 【0045】

図 7 は、図 6 の管理装置 100 の内部構成図である。管理装置 100 は、図 6 を用いて説明したとおり、実名処理部 102 と匿名処理部 104 とを有する。本図で、ライン L の左側が実名処理部 102 に該当し、右側が匿名処理部 104 に該当する。ユーザ情報管理部 136 は、ユーザの実認証情報や性別、年齢、所属などのユーザ属性を新たに受け付けユーザ情報格納部 138 に登録し、更新や削除を行う。ユーザ情報格納部 138 は、例えば実ユーザ ID に対応付けて実認証情報やユーザ属性を保持する。認証部 120 は、クライアント装置 200 からユーザ ID やパスワードを受け付け、ユーザの認証をユーザ情報格納部 138 に保持されているデータを参照して行う。実名による認証に成功した場合、認証部 120 はその旨を匿名情報生成部 106 に通知する。もちろん、認証部 120 は、認証局が発行したユーザ証明書に基づいて、認証処理を行ってもよい。要は、認証部 120 は、ユーザを直接的に特定可能な情報を利用して、ユーザの認証を行えばよい。

40

50

## 【0046】

匿名情報生成部106は、匿名ID管理部122、匿名プロキシ証明書生成部123、匿名プロキシ証明書格納部124、認証要求部128、および匿名IDテーブル126を有する。匿名IDテーブル126は、複数の匿名ユーザの情報、すなわち匿名情報を保持する。匿名IDテーブル126におけるデータ構造は任意であるが、匿名情報に加えて識別情報（以下、単に「匿名ID」という）と、その匿名情報を使用中であることを示す使用フラグとを含む。

## 【0047】

実名による認証が成功したことを認証部120から受け付けると、匿名ID管理部122は、匿名IDテーブル126の利用フラグを参照して、未使用の匿名情報を選択する。そして、匿名ID管理部122は、選択した匿名情報を匿名IDテーブル126から読み込み、匿名プロキシ証明書生成部123に出力するとともに、匿名プロキシ証明書の生成を指示する。

10

## 【0048】

匿名プロキシ証明書生成部123は、図2を用いて説明した匿名プロキシ証明書620を生成し、匿名プロキシ証明書格納部124に格納する。認証要求部128は、匿名プロキシ証明書を利用してアプリケーション提供装置300に認証処理を要求する。アプリケーション提供装置300への認証が成功した場合、認証要求部128は、その旨を処理内容受付部150に通知する。詳細は後述するが、その通知を受けて、処理内容受付部150は、クライアント装置200からジョブを受け付ける。

20

## 【0049】

また、匿名ID管理部122は、匿名プロキシ証明書生成部123に匿名プロキシ証明書の生成を指示する一方で、選択した匿名情報とユーザとを対応付けることを匿名情報管理部130に指示する。匿名情報管理部130は、実ユーザと匿名ユーザとをマッピングするマッピング処理部132と、マップファイルを保持するマッピングテーブル134とを有する。具体的には、マッピング処理部132は、匿名ID管理部122から匿名IDを受け付け、実ユーザIDと匿名IDとを対応付けてマップファイルとしてマッピングテーブル134に登録する。これにより、実際のユーザと匿名ユーザとが対応付けられるので、管理装置100はクライアント装置200に対しては実名で処理を行い、アプリケーション提供装置300および計算機400に対しては匿名で処理を行うことができる。つまり、管理装置100は、実ユーザに対する処理と匿名ユーザに対する処理とを相互に変換可能である。

30

## 【0050】

属性情報管理部108は、図4を用いて説明した匿名属性証明書636を生成し、例えばジョブが有効な期間に渡り、管理する。属性情報管理部108は、属性証明書発行部140、匿名属性証明書発行部142、匿名属性証明書格納部144、属性リストテーブル146、および属性応答部148を有する。属性証明書発行部140は、ユーザ情報格納部138に保持されているユーザ属性に基づいて、図4を用いて説明したユーザ属性証明書634を発行する。匿名属性証明書発行部142は、そのユーザ属性証明書634に基づいて使用中の匿名ID毎の匿名属性証明書636を発行して、匿名属性証明書格納部144に格納する。

40

## 【0051】

具体的には、匿名属性証明書発行部142は、マッピングテーブル134に保持されているマップファイルを参照して、使用中の匿名IDに対応付けられた実ユーザIDを特定する。そして、匿名属性証明書発行部142は、特定した実ユーザIDのユーザ属性証明書634の提供を属性証明書発行部140に要求する。その要求に応じて、属性証明書発行部140は、ユーザ情報格納部138を参照して、指定された実ユーザIDで特定されるユーザのユーザ属性に基づいて、ユーザ属性証明書634を発行する。匿名属性証明書発行部142は、こうして発行されたユーザ属性証明書634に基づいて、匿名IDに対応付け、例えばユーザ属性証明書634に保持されている属性を、更に上位概念の属性に

50

変換し匿名属性証明書 6 3 6 を生成する。

【0052】

属性応答部 1 4 8 は、アプリケーション提供装置 3 0 0 からの要求に応じて、匿名属性証明書格納部 1 4 4 に保持されている匿名属性証明書 6 3 6 をアプリケーション提供装置 3 0 0 に提供する。属性応答部 1 4 8 は、匿名属性証明書 6 3 6 全体をアプリケーション提供装置 3 0 0 に提供してもよいし、匿名属性証明書 6 3 6 の一部を要求に応じて、その都度アプリケーション提供装置 3 0 0 に提供してもよい。属性リストテーブル 1 4 6 は、アプリケーション提供装置 3 0 0 に提供可能な属性のリストを保持する。そして、アプリケーション提供装置 3 0 0 に属性リストの提供を要求された場合、属性応答部 1 4 8 は属性リストテーブル 1 4 6 から属性リストを読み込んで、アプリケーション提供装置 3 0 0 に提供する。アプリケーション提供装置 3 0 0 は、その属性リストに基づいて、ジョブの実行条件を満たすために必要な属性を属性応答部 1 4 8 に問い合わせてもよい。

10

【0053】

また、匿名属性証明書格納部 1 4 4 は、属性毎に、提供に際してユーザの許可が必要かどうかを指定する提供フラグを有する。属性応答部 1 4 8 は、その提供フラグにユーザの許可が必要であることを示すフラグが保持されている場合、その属性をアプリケーション提供装置 3 0 0 に提供してよいか否かをクライアント装置 2 0 0 に問い合わせる。また、提供フラグにユーザの許可は不要であることを示すフラグが保持されている場合、ユーザに問い合わせることなく自動的にその属性をアプリケーション提供装置 3 0 0 に提供する。これにより、属性レベルの情報でさえも、ユーザの個人情報が管理装置 1 0 0 の後段に存在するアプリケーション提供装置 3 0 0 や計算機 4 0 0 に必要以上に流出することを防止できる。

20

【0054】

他の例では、属性応答部 1 4 8 は、匿名属性証明書格納部 1 4 4 に保持されている属性をそのままアプリケーション提供装置 3 0 0 に送信するのではなく、アプリケーション提供装置 3 0 0 からの「ユーザは××学会の会員ですか？」という問いに対して、「はい／いいえ」のどちらかで応答するような間接的な方法で属性を提供してもよい。具体的には、属性応答部 1 4 8 とアプリケーション提供装置 3 0 0 との間で、応答のためのコマンドや X M L (eXtensible Markup Language) におけるタグなどを定義しておき、それらを利用して実行条件の交渉が行われる。つまり、属性応答部 1 4 8 は、匿名性を保ちつつ、匿名化されたユーザに関する情報を提供する機能を有すればよい。このような方法により、グリッドシステム 5 0 0 は更に強固な匿名性を実現し、ユーザの個人情報の隠蔽を完全なものにできる。

30

【0055】

前述の認証要求部 1 2 8 が、認証に成功した場合、処理内容受付部 1 5 0 は、ジョブをクライアント装置 2 0 0 から受け付ける。例えば、処理内容受付部 1 5 0 は、ジョブを受け付けるための表示画面を形成するための例えば H T M L (HyperText Markup Language) などの文書記述言語で構成された画面情報をクライアント装置 2 0 0 に送信する。そして、処理内容受付部 1 5 0 は、その表示画面を介して入力されたジョブを、クライアント装置 2 0 0 から受け付ける。処理内容受付部 1 5 0 は、受け付けたジョブを実ユーザ I D に対応付けてスケジューリング処理部 1 5 2 に出力する。

40

【0056】

スケジューリング処理部 1 5 2 は、ジョブをアプリケーション提供装置 3 0 0 に要求する順序や時期などを、例えばその時のグリッド環境における計算機 4 0 0 の稼働状態や、ユーザとの契約上の優先度などに基づいて計画する。そして、スケジューリング処理部 1 5 2 は、ジョブの実行計画を実ユーザ I D に対応付けてジョブ管理部 1 1 0 に出力する。

【0057】

ジョブ管理部 1 1 0 は、マッピングテーブル 1 3 4 を参照して、実ユーザ I D に対応付けられた匿名 I D を特定し、特定した匿名 I D に対応付けてジョブを処理要求部 1 5 4 に出力する。処理要求部 1 5 4 は、匿名 I D とジョブとを対応付けてアプリケーション提供

50

装置 300 に送信し、そのジョブの実行を要求する。この要求を受けて、アプリケーション提供装置 300 は、前述した属性応答部 148 に対して実行条件の交渉のため、属性の問い合わせを行う。

#### 【0058】

処理結果受付部 156 は、アプリケーション提供装置 300 から匿名 ID に対応付けられた計算結果を受け付け、ジョブ管理部 110 に供給する。ジョブ管理部 110 は、その計算結果を匿名 ID に対応付けてファイル管理部 158 に供給する。そして、ジョブ管理部 110 は、マッピングテーブル 134 を参照して匿名 ID に対応付けられた実ユーザ ID を特定し、そのユーザのクライアント装置 200 にジョブが完了したことを通知するメッセージを送信する。

10

#### 【0059】

ファイル管理部 158 は、計算結果を匿名 ID に対応付けて短期保存データ格納部 162 に格納し、実ユーザ ID に対応付けて長期保存データ格納部 160 に格納する。ファイル管理部 158 は、短期保存データ格納部 162 に格納されている計算結果を所定の時間が経過した後、強制的に削除する。例えば、ファイル管理部 158 は、ジョブが完了したことを契機として、計算結果を削除してもよい。ここで、処理結果受付部 156 が受け付け、ジョブ管理部 110 がファイル管理部 158 に供給する計算結果は、ジョブに対する最終的な計算結果でもよいし、一連のジョブを実行する過程で、生成された途中の計算結果（以下、単に「テンポラリ・ファイル」という）でもよい。また、処理結果受付部 156 が受け付ける計算結果およびテンポラリ・ファイルを総称して、「受信ファイル」という。

20

#### 【0060】

処理結果受付部 156 が受け付ける受信ファイルには、テンポラリ・ファイルであるか、最終的な計算結果であるかを指定するファイル属性情報が対応付けられている。そして、ファイル管理部 158 は、ファイル属性情報に基づいて、受信ファイルを長期保存データ格納部 160 または短期保存データ格納部 162 に振り分けて格納する。図 6 の計算機 400 の提供部 408 は、計算結果にファイル属性情報を対応付けてアプリケーション提供装置 300 に提供する。これにより、処理結果受付部 156 は、ファイル属性情報の対応付けられた受信ファイルを受け付けることができる。

#### 【0061】

例えば、グリッド環境における複数の計算機 400 を利用してジョブを行う場合、ファイル管理部 158 は、それぞれの計算機 400 における計算結果を匿名 ID およびジョブにおける変数名などに対応付けて短期保存データ格納部 162 に格納する。そして、その計算結果を利用する計算機 400 から要求された場合、ファイル管理部 158 は、要求された計算結果を短期保存データ格納部 162 から読み込み、処理結果受付部 156 を介して計算機 400 に提供する。本図では、管理装置 100 と計算機 400 とは直接通信は行わず、アプリケーション提供装置 300 を介して行う形態を図示している。このように、短期保存データ格納部 162 は、一連のジョブを完了する際に生じる一時的な計算結果を格納するための一時格納エリアとして、グリッド環境における各計算機 400 により利用される。これにより、匿名性を確保しつつ、計算機 400 において生成された計算結果やテンポラリ・ファイルを再利用することが可能になる。

30

40

#### 【0062】

長期保存データ格納部 160 は、最終的に得られたジョブの計算結果を実ユーザ ID に対応付けて保持する。これにより、ジョブ管理部 110 は、ユーザに要求された場合に、長期保存データ格納部 160 に保持されている計算結果をクライアント装置 200 に提供することができる。

#### 【0063】

図 8 は、図 6 を用いて説明したグリッドシステム 500 における各装置間の処理のシーケンスの一例を示す図である。本図で、アプリケーション提供装置 300 および計算機 400 は、まとめて記述している。以下、それらを単に計算機 400 として説明する。まず

50

、クライアント装置 200 は、実名でジョブの処理を要求する (S 10)。管理装置 100 は、実認証情報に基づいてユーザの認証を行う (S 12)。認証に成功した場合、管理装置 100 は、匿名プロキシ証明書を生成し (S 14)、計算機 400 に認証処理を要求する (S 16)。

【0064】

計算機 400 は、匿名プロキシ証明書を利用して認証処理を行う (S 18)。認証に成功した場合、計算機 400 は、ユーザの属性情報が必要か否かを判断する (S 20)。属性情報が必要な場合 (S 20 の Y)、計算機 400 は管理装置 100 に属性情報を要求する (S 22)。管理装置 100 は、図 4 を用いて説明した匿名属性証明書 636 を参照して、要求された属性情報を選択し (S 24)、計算機 400 に送信する (S 26)。ここで、本実施の形態の管理装置 100 は、ユーザに予め許可されている属性情報のみを、自動的に計算機 400 に送信する。このため、計算機 400 がユーザに許可されていない属性情報を要求した場合、必要な属性情報が得られていないことになる。このために次のステップ 28 が設けられている。計算機 400 は、必要な属性情報を全て取得できたか否かを判断する (S 28)。必要な属性情報が不足している場合 (S 28 の N)、計算機 400 は実行条件を管理装置 100 に通知する (S 30)。そして、管理装置 100 は、その実行条件をクライアント装置 200 に通知する (S 32)。

10

【0065】

ユーザはその実行条件に応じて、属性情報の送信の許可を指定する情報を管理装置 100 に送信する (S 34)。許可された場合 (S 36 の Y)、管理装置 100 はその属性情報を計算機 400 に送信する (S 40)。また、拒否された場合 (S 36 の N)、管理装置 100 は拒否されたことを示す情報を計算機 400 に送信する (S 38)。そして、計算機 400 は、再度、必要な属性情報を全て取得したか否かを判断する (S 42)。必要な情報を取得できなかった場合 (S 42 の N)、計算機 400 はジョブを実行できないことを示すエラーメッセージを管理装置 100 に送信する (S 44)。そして、管理装置 100 は、そのエラーメッセージをクライアント装置 200 に送信する (S 46)。

20

【0066】

また、ステップ 42 で、必要な情報を全て取得できた場合 (S 42 の Y)、計算機 400 は依頼されたジョブを実行し (S 48)、計算結果を管理装置 100 に送信する (S 50)。そして、管理装置 100 は、その計算結果をクライアント装置 200 に送信する (S 52)。また、ステップ 20 で、属性情報が必要無い場合 (S 20 の N)、計算機 400 はジョブを実行する (S 48)。また、ステップ 28 で、必要な情報を全て取得した場合 (S 28 の Y)、計算機 400 はジョブを実行する (S 48)。

30

【0067】

以上、本発明を実施の形態をもとに説明した。この実施の形態は例示であり、それらの各構成要素や各処理プロセスの組合せにいろいろな変形例が可能なこと、またそうした変形例も本発明の範囲にあることは当業者に理解されるところである。

【図面の簡単な説明】

【0068】

【図 1】図 1 (a) は、従来のグリッドシステムの構成図であり、図 1 (b) は、プロキシ証明書ファイルのデータ構造と生成処理を説明するための図である。

40

【図 2】第 1 の実施の形態に係るグリッドシステムの構成図である。

【図 3】第 1 の要素技術である「複数の匿名情報を利用して、ユーザ毎に図 2 の匿名プロキシ証明書を生成する技術」を説明するための図である。

【図 4】第 2 の要素技術である「匿名性を保ちながらユーザの属性を提供する技術」を説明するための図である。

【図 5】第 3 の要素技術である「匿名性を保ちながら過去の計算結果を使用する、もしくは他のユーザに公開するといったデータの再利用を可能にする技術」を説明するための図である。

【図 6】第 2 の実施の形態に係るグリッドシステムの構成図である。

50

【図 7】図 6 の管理装置の内部構成図である。

【図 8】図 6 を用いて説明したグリッドシステムにおける各装置間の処理のシーケンスの一例を示す図である。

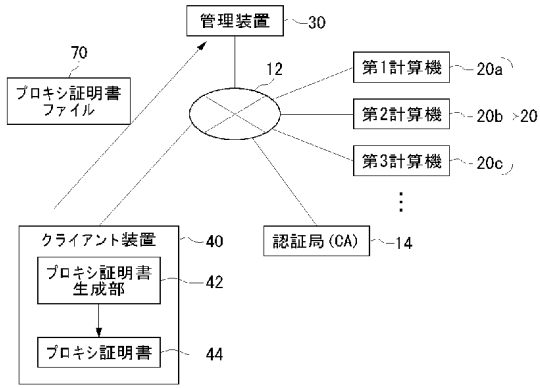
【符号の説明】

【0069】

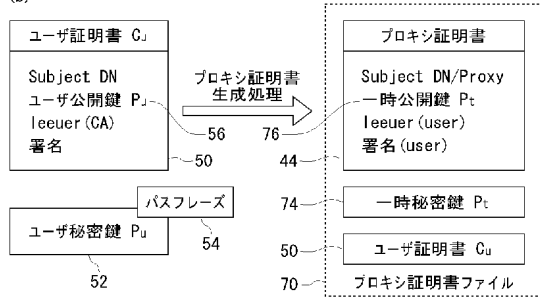
10    10    グリッドシステム、12    ネットワーク、14    認証局、20    計算機、30    管理装置、40    クライアント装置、42    プロキシ証明書生成部、44    プロキシ証明書、50    ユーザ証明書、52    ユーザ秘密鍵、54    パスフレーズ、56    ユーザ公開鍵、70    プロキシ証明書ファイル、74    一時秘密鍵、76    一時公開鍵、94    長期保存データ、96    短期保存データ、100    管理装置、102    実名処理部、104    匿名処理部、106    匿名情報生成部、108    属性情報管理部、110    ジョブ管理部、112    一時格納部、114    削除部、120    認証部、122    匿名ID管理部、123    匿名プロキシ証明書生成部、124    匿名プロキシ証明書格納部、126    匿名IDテーブル、128    認証要求部、130    匿名情報管理部、132    マッピング処理部、134    マッピングテーブル、136    ユーザ情報管理部、138    ユーザ情報格納部、140    属性証明書発行部、142    匿名属性証明書発行部、144    匿名属性証明書格納部、146    属性リストテーブル、148    属性応答部、150    処理内容受付部、152    スケジューリング処理部、154    処理要求部、156    処理結果受付部、158    ファイル管理部、160    長期保存データ格納部、162    短期保存データ格納部、200    クライアント装置、202    処理要求部、204    データ格納部、206    結果受付部、208    結果格納部、210    表示処理部、250    汎用データ提供装置、252    汎用データ格納部、300    アプリケーション提供装置、302    匿名認証部、304    指示部、306    アプリケーション格納部、308    中継部、310    削除部、312    一時格納部、400    計算機、402    処理要求受付部、404    実行部、406    取得部、408    提供部、410    一時格納部、412    削除部、500    グリッドシステム、600    グリッドシステム、610    管理装置、612    認証部、614    ユーザ情報格納部、616    プロキシ証明書生成部、618    匿名情報格納部、620    匿名プロキシ証明書、630    ユーザ、632    サーバ、634    ユーザ属性証明書、636    匿名属性証明書。

【 例 1 】

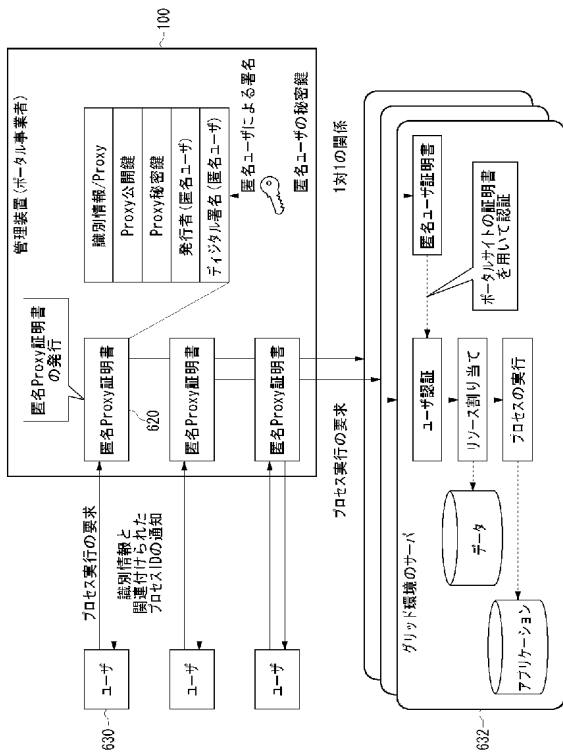
(a)



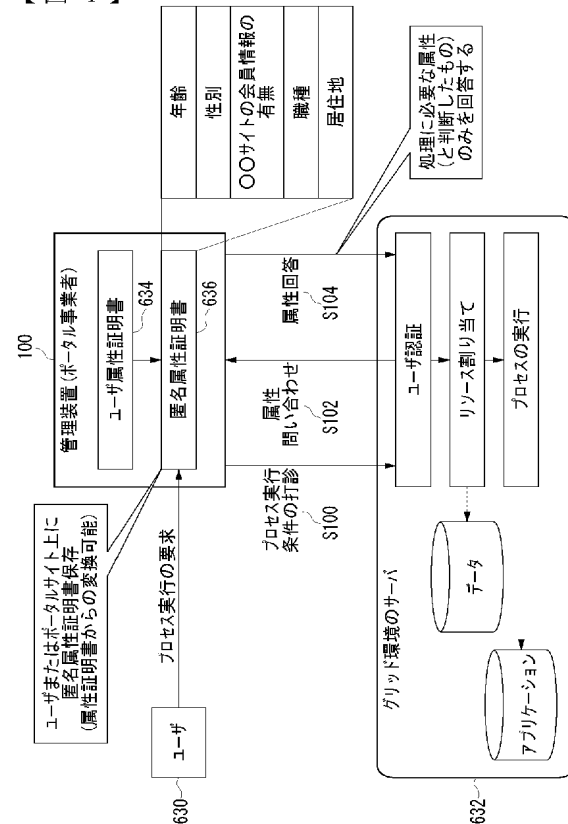
(b)



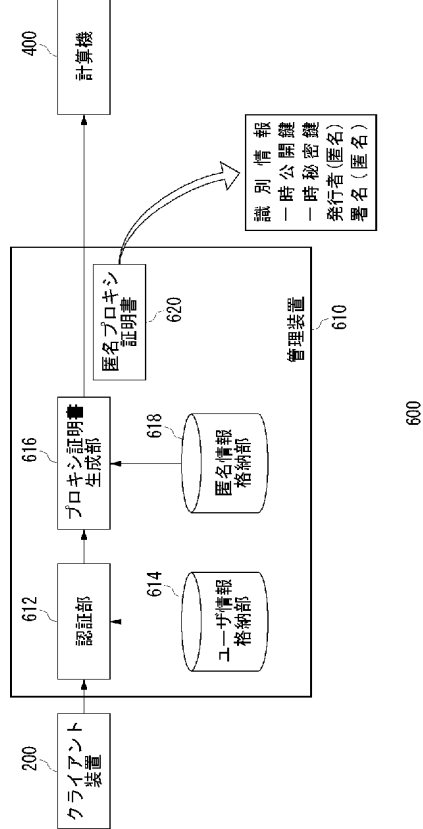
【 例 3 】



【图 4】

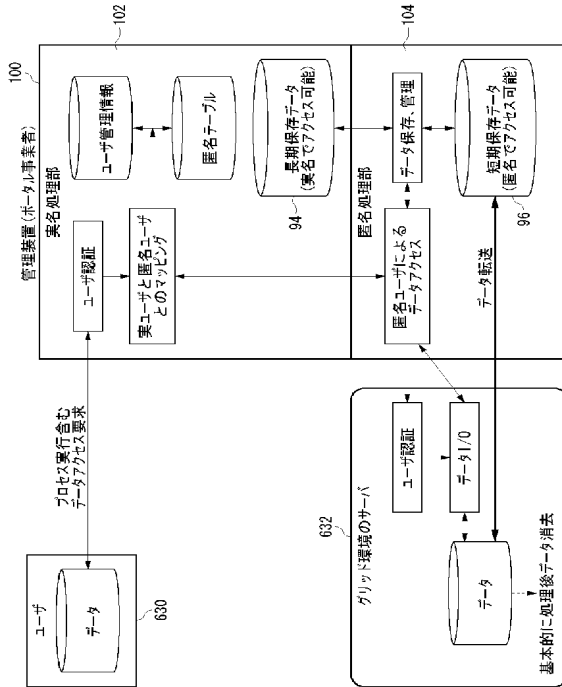


【図 2】

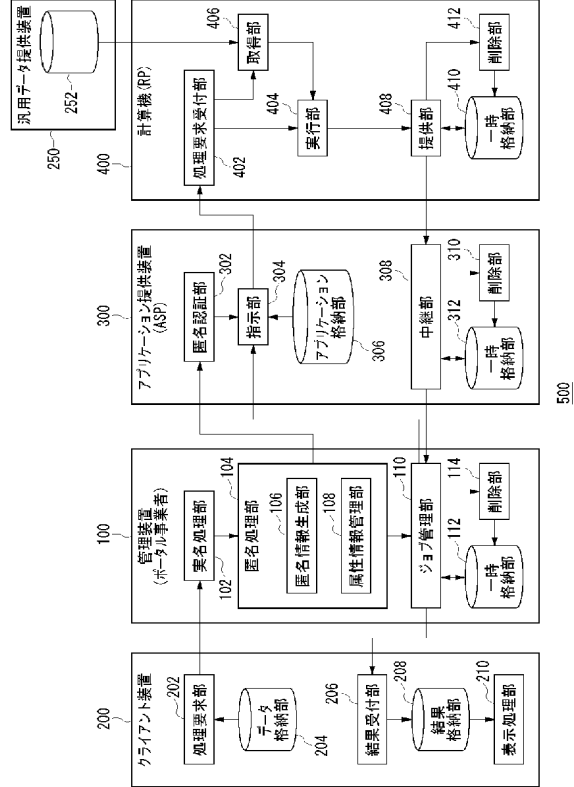




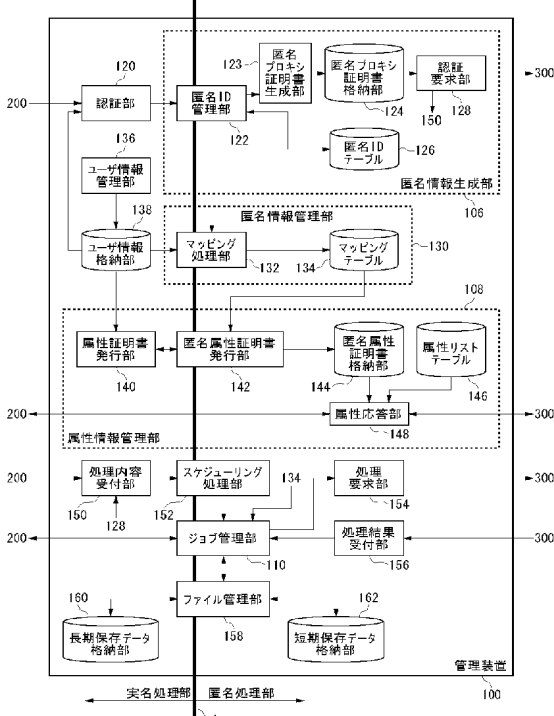
【図 5】



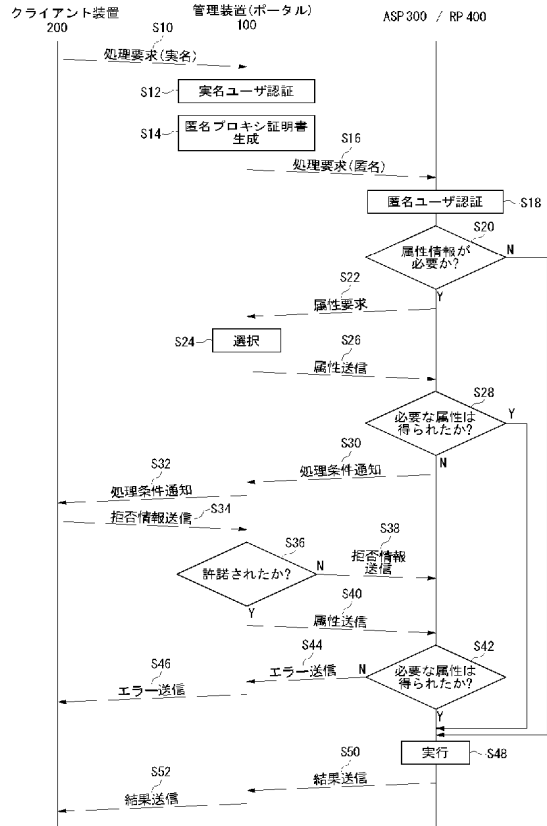
【図 6】



【図 7】



【図 8】



---

フロントページの続き

- (72)発明者 伊藤 智  
茨城県つくば市東 1-1-1 独立行政法人産業技術総合研究所つくばセンター内
- (72)発明者 高木 浩光  
茨城県つくば市東 1-1-1 独立行政法人産業技術総合研究所つくばセンター内
- (72)発明者 森尻 智昭  
東京都港区芝浦一丁目 1 番 1 号 東芝ソリューション株式会社内
- (72)発明者 才所 敏明  
東京都港区芝浦一丁目 1 番 1 号 東芝ソリューション株式会社内
- Fターム(参考) 5B285 AA04 CA43 CB47 CB51 CB91  
5J104 KA01 PA07

**PAT-NO:** JP02006301831A  
**DOCUMENT-IDENTIFIER:** JP 2006301831 A  
**TITLE:** MANAGEMENT DEVICE  
**PUBN-DATE:** November 2, 2006

**INVENTOR-INFORMATION:**

<b>NAME</b>	<b>COUNTRY</b>
TANAKA, YOSHIO	N/A
SEKIGUCHI, TOMOTSUGU	N/A
ITO, SATOSHI	N/A
TAKAGI, HIROMITSU	N/A
MORIJIRI, TOMOAKI	N/A
SAISHIYO, TOSHIAKI	N/A

**ASSIGNEE-INFORMATION:**

<b>NAME</b>	<b>COUNTRY</b>
NATIONAL INSTITUTE OF ADVANCED INDUSTRIAL & TECHNOLOGY	N/A
TOSHIBA SOLUTIONS CORP	N/A

**APPL-NO:** JP2005120627  
**APPL-DATE:** April 19, 2005

**INT-CL-ISSUED:**

<b>TYPE</b>	<b>IPC DATE</b>	<b>IPC-OLD</b>
-------------	-----------------	----------------

IPCP	G06F21/20	20060101 G06F021/20
------	-----------	---------------------

IPFC

G09C1/00 20060101 G09C001/00

**ABSTRACT:**

PROBLEM TO BE SOLVED: To provide a technique facilitating authentication processing in a grid environment and a technique attaining a secure grid environment.

SOLUTION: A grid system 600 is connected to a client device 200 through SSL and performs authentication based on a user's ID or password. When the authentication is successful, an authentication part 612 instructs generation of an anonymous proxy certificate to a proxy certificate generation part 616. The proxy certificate generation part 616 reads preliminarily registered anonymous user information from an anonymous information storage part 618, and generates an anonymous proxy certificate 620 based on the anonymous information. The management device 610 performs authentication processing to a computer 400 using the anonymous proxy certificate 620 to make the computer execute jobs. The computer 400 accepts the validity of the anonymous proxy certificate 620 by trusting the management device 610. By using the anonymous proxy certificate in this way, transfer of personal information of a user to the computer 400 can be prevented.

COPYRIGHT: (C)2007,JPO&INPIT